What is claimed is:

1. A method for a network, comprising:

determining suspicious network activity on the network;

receiving an initial packet from a first machine for establishing a communication session between the first machine and a second machine;

sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and

establishing the communication session between the first and second machines after a valid response is received to the test.

2. The method of claim 1 further comprising responding to the initial packet from the first machine by sending a response packet to the first machine encoding a connection state for establishing the communication session.

3. The method of claim 2 wherein the initial packet is a SYN packet in accord with the TCP protocol and the response packet is a SYN ACK packet in accord with the TCP protocol.

4. The method of claim 3, wherein the SYN ACK comprises a number encoding a first address for the first machine on the network, and a second address for the second machine on the network.

5. The method of claim 2, wherein the connection state of the response packet comprises a number encoding a first address for the first machine on the

network, a second address for the second machine on the network, and a secret unknown to the first machine to facilitate validating an acknowledgement from the first machine responsive to the response packet.

6. The method of claim 1, further comprising:

receiving an acknowledgement packet from the first machine responsive to the response packet;

decoding a tentative connection state information from the acknowledgement packet; and

determining if the tentative connection state information is valid.

7. The method of claim 1, further comprising:

preparing a web page embodying the test; and

said sending the test to the first machine including sending the web page to a networking application program of the first machine, the networking application program operative to receive and display the web page.

8. The method of claim 1, wherein the test is embodied within a web page.

9. The method of claim 1, further comprising:

monitoring by a monitoring device of attempts to establish communication sessions with the second machine;

wherein the establishing the communication session between the first and second machines includes the monitoring device establishing a first connection between

the monitoring device and the first machine, and the monitoring device establishing a second connection between the monitoring device and the second machine.

10. The method of claim 1, further comprising:

monitoring by a monitoring device of attempts to establish communication sessions with the second machine;

wherein the establishing the communication session between the first and second machines includes the monitoring device storing an identifier for the first machine in a list identifying machines that have provided the valid response.

11. A method for a monitoring device to facilitate communication between a client and a protected server, comprising:

receiving a first packet from the client to begin a handshake for establishing a first network connection between the client and the intermediary;

sending a second packet to the client to acknowledge the first packet;

receiving a third packet from the client acknowledging the second packet;

receiving a data access request from a networking application program of the client; and

sending a test to the networking application program, the test having at least one characteristic making the test resistant to automatic answering of the test.

12. The method of claim 11, further comprising:

receiving a response to the test from the client;

determining the response comprises a valid answer to the test;

establishing a second network connection between the monitoring device and the protected server; and

facilitating communication between the client and the protected server.

13. The method of claim 11, wherein the monitoring device does not allocate resources for tracking a state information for establishing the first network connection and instead encodes the state information within the second packet.

14. The method of claim 11, wherein the third packet encodes a known alteration of the state information.

15. The method of claim 11, wherein the data access request is a GET request formatted with respect to HyperText Transport Protocol (HTTP).

16. The method of claim 11, wherein the networking application program includes a web browser, and the test comprises a web page incorporating the test.

17. A system, comprising:

a protected server responsive to network connection requests;

a client machine seeking to establish communication with the protected server; and

a monitoring device communicatively interposed between the protected server and the client machine, wherein the monitoring device is configured to send a test resistant to automatic answering to the client machine, and to facilitate establishing the

client machine communication with the protected server if a valid response to the test is received by the monitoring device.

18. The system of claim 17, wherein the monitoring device is further configured to perform:

receiving an initial packet from the client machine for establishing a communication session; and

responding to the initial packet by sending a response packet to the client machine encoding a connection state for establishing the communication session.

19. An article comprising a machine-accessible media having associated data, wherein the data, when accessed, results in a machine communicatively coupled with a network performing:

determining suspicious network activity on the network;

receiving an initial packet from a first machine for establishing a communication session between the first machine and a second machine;

sending a test to the first machine, the test having at least one characteristic making the test resistant to automatic answering of the test; and

establishing the communication session between the first and second machines after a valid response is received to the test.

20. The article of claim 19 wherein the machine-accessible media further includes data, when accessed, results in the machine performing:

responding to the initial packet from the first machine by sending a response packet to the first machine encoding a connection state for establishing the communication session.

21. An article comprising a machine-accessible media having associated data for a monitoring device to facilitate communication between a client and a protected server, wherein the data, when accessed, results in a machine performing:

receiving a first packet from the client to begin a handshake for establishing a first network connection between the client and the intermediary;

sending a second packet to the client to acknowledge the first packet;

receiving a third packet from the client acknowledging the second packet;

receiving a data access request from a networking application program of the client; and

sending a test to the networking application program, the test having at least one characteristic making the test resistant to automatic answering of the test.

22. The article of claim 21 wherein the machine-accessible media further includes data, when accessed, results in the machine performing:

receiving a response to the test from the client;

determining the response comprises a valid answer to the test;

establishing a second network connection between the monitoring device and the protected server; and

facilitating communication between the client and the protected server.